

Ryan Miller  
Chief Operating Officer  
10813 S. River Front Pkwy, Suite 500  
South Jordan, Utah 84095  
(801) 878-3200



**BROADWEAVE**  
NETWORKS

February 27, 2009

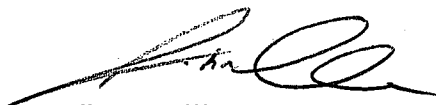
Marlene H. Dortch  
Secretary  
Federal Communications Commission  
445 12<sup>th</sup> Street, S.W., Suite TW-A325  
Washington D.C. 20554

RE: *CPNI Certification for Data Pertaining to 2008 – EB Docket No. 06-36*

Dear Ms. Dortch:

Enclosed is Broadweave Networks annual CPNI Certification for data pertaining to 2008. Please do not hesitate to contact me if you have any questions.

Sincerely,



Ryan Miller  
Chief Operating Officer  
Broadweave Networks

**Annual 47 C.F.R. § 64.2009(e) CPNI Certification  
EB Docket 06-36**

Annual 64.2009(e) CPNI Certification for year 2008

Date Filed: February 27, 2009

Name of Company Covered by This Certification: Broadweave Networks

Form 499 Filer ID: 826588

Name of Signatory: Ryan Miller

Title of Signatory: Chief Operating Officer


I, Ryan Miller, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Federal Communications Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompany statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in Section 64.2001 *et seq.* of the Federal Communications Commission's rules.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court systems, or at the Federal Communications Commission against data brokers) against data brokers in the past year. Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI, and what steps companies are taking to protect CPNI.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI (number of customer complaints a company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category or complaint, *e.g.*, instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view information).

Signed: \_\_\_\_\_



**Accompanying Statement of Annual CPNI Compliance Certification**

The company has taken any or all of the following actions to protect against the unlawful disclosure of CPNI:

Employee Training and Discipline

- Trained all employees and personnel as to when they are and are not authorized to use CPNI
- Instituted an express disciplinary process for unauthorized use of CPNI

Sales and Marketing Campaign Approval

- Guaranteed that all sales and marketing campaigns are approved by management

Record-Keeping Requirements

- Established a system to maintain a record of all sales and marketing campaigns that use their customers' CPNI, including marketing campaigns of affiliates and independent contractors
- Ensured that these records include a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as part of the campaign
- Made certain that these records are maintained for a minimum of one year

Establishment of a Supervisory Review Process

- Established a supervisory review process for all outbound marketing situations
- Certified that under this review process, all sales personnel obtain supervisory approval of any proposed outbound marketing request for customer approval

Opt-In

- Guaranteed that the company only disclosed CPNI to agents, affiliates, joint venture partners, independent contractors or to any other third parties only after receiving "opt-in" approval from a customer
- Verified that the company enters into confidential agreements with joint venture partners, independent contractors or any other third party when releasing CPNI

Opt-Out Mechanism Failure

- Establish a protocol through which the company will provide the FCC with written notice within five (5) business days of any instance where opt-out mechanisms do not work properly

Compliance Certificates

- Executed a statement, signed by an officer, certifying that he or she has personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the FCC's CPNI rules and regulations

- Executed a statement detailing how operating procedures ensure compliance with the FCC's CPNI rules and regulations
- Executed a summary of all customer complaints received in the past year concerning unauthorized release of CPNI

## Customer Authentication Methods

- Instituted customer authentication methods to ensure adequate protection of customers CPNI in accordance with the following methods:
  - Disclosure of CPNI in response to a customer providing a pre-established password,
  - Disclosure of CPNI to the customer's address or phone number of record, and
  - Access to CPNI if a customer presents a valid photo identification at the company's retail location

## Customer Notification of CPNI Changes

- Established a system under which a customer is notified of any changes to CPNI including CPNI access in the following circumstances
  - Password modification
  - A response to a carrier-designated back-up means of authentication
  - Online account changes, or
  - Address of record change or creation

## Notification of Law Enforcement and Customer of Unauthorized Access

- Established a protocol under which the appropriate law enforcement agency is notified of any unauthorized access to customer CPNI
- Ensured that all records of any discovered CPNI breaches are kept for a minimum of two years